Application of Cryptography in Digital Rights Management

Adhika Sigit Ramanto - 13512060
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13512060@stei.itb.ac.id

***Abstract*— this essay was made to explain how an application of number theory could be used to protect digitial contents for the purpose of conserving one's rights of a work, or product. Cryptography can be used on most of content types, especially entertainments that can nowadays be downloaded from various sources, and it is used to control the use of said downloaded content to the rights owners' intent. The cryptographic techniques to protect digitized contents are commonly known as Digital Rights Management and it encompasses interests in a broad range of studies, including discrete mathematics.**

***Index Terms*— Number Theory, Cryptogaphy, Digital Rights, Copyright**

I. INTRODUCTION

1.1. Prevalence of Digital Content

Since the dawn of mass distributed media, there has been attemptsat acquiring them illegally, the motive of the perpetrators can usually be simplified into avoiding the "creative costs" outside of the price of the medium itself, this cost that they are trying to avoid is most of the time the value determined by the content that the consumers want . If we are to observe a book, which is the first medium for entertainment that is mass-produced and mass-distribute, acquiring it illegally would mean to hard-copy the contents without actually having a sum of money that will eventually fall into the authors' pockets. But doing this to a book would have been a cumbersome exercise in the past because the perpetrator would have to have approximately the same amount of writing space with the original book itself.

With the rapid advance in technology, most notably in the last fifty years, the core nature of a lot of content itself has changed, namely with digital innovations in information technology. We have also acquired numerous new ways to store content e.g. the Compact Disc (CD) , Digital Versatile Disc (DVD), etc. But perhaps the most important change we, as the consumers, tend to take lightly is how a content can be treated when digitized or created digitally.

Looking at a more recent time frame, it can be easily observed that most business models, mainly the ones in the field of entertainment, has taken a departure to the digital world and changes the way they create and distribute content to a point where the consumer doesn't need to move an inch in front of their computer, provided that they are connected to the internet. This newer business model has even impoverished the ones that hasn't moved on from the physical realm. Music can now simply be downloaded from iTunes or Amazon, even with packaged contents not available physically. Whole movies can now be streamed in its entirety online on Netflix, a company that has evidently obliterated the life of DVD rental company Blockbuster. Games are much cheaper and easier to store when bought online from Steam. Even in the midst of college nowadays most students prefer to bring their whole collection of eBooks in their tablets rather than carrying a 1000-page thick book for a single subject.

In the past, we might observe that a single pirate (a commonly used term to describe a perpetrator of digital theft) can only produce a finite amount of illegal copies with the limitation of physical storage, not to forget that the quality of the content itself tend to deteriorate with each copy. Nowadays, content creators and copyright holders face the threat in which a single pirate can distribute an infinite amount of perfectly reproduced copies with minimum effort with the prevalence of completely digital distribution of contents.

1.2. Digital Rights Management

After observing what the pervasiveness of digital content delivery and how far easier it is for a single entity to distribute a content with the same quality, one might question how the companies with digital content deliveries are still holding up and making profits, some of it even becoming the most valuable companies in the world in recent years. One of the tech that prevents these companies from collapsing is called Digital Rights Management (DRM).

DRM was first implemented to compact discs in the year 2002 where a group of record companies ship CDs with contents that can't be played if it is copied outside the CD. Sony BMG created a more obtrusive and controversial form of DRM where the CD will install a software on the computer without the consumer's consent. In initial stage, digital rights protection mainly solves the unauthorized duplication problem of the digital product by safeencryption technique. It only distributes the digital product tothe user who has already paid for it. Nowadays, as a comprehensive digital content management technology, DRM has covered all kinds of aspects of the digital content, including creating, description, marking, exchange, protection, and usage.

Though the use of a DRM system is crucial to the well-being of companies in the field, some implementations of it has been controversial to a number of communities with concerns to fairness of use and the rise of the free market. Even some content creators has taken a stance against DRM for they deem the actual purposes can be distorted into a very limiting freedom of use for the consumer considering the companies usually set the price quite near the actual price point of the same content in its physical copy. One very recent instance of how DRM can make or break a business is how Microsoft's Xbox One gaming console manages the games bought either online or in discs. The DRM system limits the user into locking the game into users in one console, without the ability to retract the lock and give it to other players.

II. Theories

2.1 Number Theory

In mathematics, number theory is a field that concerns itself with the properties of natural numbers, integers, or rational numbers, delving in questions such as "If n is a composite number, how can we factorize it?" or "How closely can we approximate a given irrational number by rational numbers which are not too complicated?" Integers are defined as a number that doesn't have a fractional or decimal component, as opposed to real numbers.

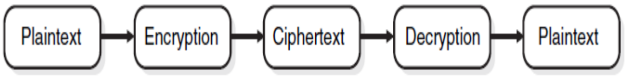
The basic rule of division for an integer is "If a divides b, there must be an integer c so that b=ac" This foundation brings us into what is called as Euclid's Algorithm, in which the first theorem states "If there are integers m and n, n>0 and m is divided by n, there must be a quotient q and remainder r where m=nq+r" An iteration of this statement is the base of finding the greatest common divisor between two integers

A better understanding of Euclidean operations and greatest common divisors can bring us to what is known as modular arithmetic and congruence. Let n be a natural number. We say that a and b are congruent modulo n if n divides a-b. We can write this as a ≅ b mod n. two numbers are congruent modulo n if and only if they leave the same remainder when they are divided by n. Congruence modulo n is an equivalence relation; the equivalence classes are called congruence classes modulo n. Deeper examinations of natural numbers and its relation to other natural numbers give way to a very wide array of sub-fields that concerns itself to a specific combination usage of intrinsic natures of integers. One of the most famous sub-field and application of number theory is cryptography.

2.2 Cryptography

In discrete mathematics, cryptography is an application of number theory. Cryptography comes from the latin words kriptos, meaning hidden, and graphein, meaning write. Cryptography is a method of storing and transferring information in a form that only those it is intended for can process to read or use. It is a science of protecting information by encoding it into an unreadable format.

The first form of cryptography emerged way before information technology rose; dating back to 4,000 years ago as hieroglyphs were invented by Egyptians and it is now considered an ancient art. As cryptography and humanity evolved, it was mainly used to pass messages through hostile environments of war, crisis, and for negotiations processes between conflicting groups of people, sending information crucial enough that it could win the war, or lose it when fallen into the opposing hands. As time went on, the encryption algorithms and the devices using them increased in complexity, new methods and algorithms are perpetually introduced, and it became an integrated part of information technology.



The process of encryption transforms plaintext into ciphertext and the process of decryption transforms ciphertext into plaintext.

Encryption is a method of transforming original data, called *plaintext*, into a form that appears to be unreadable and cannot be processed all by itself, which is called *ciphertext*. Plaintext is in a form that can be understood by a person or by a computer. When transformed into ciphertext, neither human nor machine can properly process it until it has gone through *decryption*. This enables the transmission of confidential data over insecure channels without unauthorized disclosure. When data is stored on a computer, it is usually protected by logical and physical access controls. When the same information is sent over a network, then the controls are lost, that's why we need cryptography to protect the file for itself. The process itself is usually as follows:

A system that provides a method of cryptography is referred to as a *cryptosystem* and can come in the form of hardware components or programs in software. The cryptosystem uses an encryption algorithm, and the algorithm will determine how simple or complex the process of encryption and decryption will be. Most algorithm are complex mathematical formulas that are applied in a specific sequence to the plaintext. Most encryption methods use a secret value called a *key* (usually a long string of bits), which works with the algorithm to encrypt and decrypt the text. The algorithm that dictates how enciphering and deciphering take place may be publicly known and are not what is secret about the encryption process.

The way that encryption algorithms work can be kept secret, but many of them are publicly known and well understood. The part that is secret and elusive of using a well-known encryption algorithm is the key. The key can be any value that is made up of a large sequence of random bits. However, it is not just any random number of bits crammed together. An algorithm contains a *keyspace*, which is the range of values that can be used to construct a key. The key is made up of random values within the keyspace's range. The larger the keyspace, the more available values can be used to represent different keys, and the more random keys are, the harder it is for snoopers to figure them out.

A large keyspace allows room for more possible combination of values that form keys. A good encryption algorithm uses the entire keyspace and chooses the values to make up the keys as random as possible. If a smaller keyspace were used, there would be fewer values to choose from when forming a key. This would increase an attacker's chance of figuring out the key value and deciphering the ciphertext.

The strength of a cryptosystem is determined by the algorithm, the secrecy of the key, the length of the key, initiaAation vectors, and how they all work together as a whole. Strength here is defined as the difficulty in figuring out the algorithm and key of the cryptosystem, also known as *work factor*. Finding out a key usually has a lot to do with processing an immense number of possible values in the hopes of finding the one value that can be used to decrypt a specific message (or the whole message, relative to the keyspace used). The strength correlates to the amount of necessary processing power and time it takes to break the key and figure out the algorithm used for the key itself. Most "brute force attack" approach in finding a key involves trying every key possible.

The goal of designing an encryption method is to make breaking the cipher too expensive or too time consuming. The strength of the protection mechanism should be used in correlation to the sensitivity of the data being encrypted. But even if the algorithm is very complex, there are other issues in encryption that can weaken the strength of encryption methods, such as improper protection of the key. If a user shares his key with others, the other pieces of encryption really don't matter much. To sum up, cryptography vastly depends on how the system works altogether and it is defined by the weakest link in the chain of algorithms, keyspace, formation and protection of keys.

Cryptosystems can provide *confidentiality*, meaning no unauthorized parties have access to the information. It should conserve the *integrity* of the message so that the message was not modified during process of encryption and transmission, accidentally or intentionally. The source of the message and proper identification of the sender must be preserved in *authenticity*. With a cryptosystem, the sender cannot deny sending the message, and the recipient cannot deny receiving it, in other words, it must provide *nonrepudiatio*n. Different types of information will require different priorities of these four factors. Intelligence agencies may be more concerned of the confidentiality, while financial institutions put integrity at the top of other factors.

III. Cryptography in Digital Rights Management

3.1. General application of cryptography in DRM

Having examined cryptography and how it is used to protect information, we now bring the discussion into the usage of the science and technology in the digital world. The reason why the field is called information technology is because various forms of information are all that is being sold in the digital world. Every piece of content, every track on an album, all the frames from a full movie, and every word on an eBook is fundamentally bits of the same type of information that is transmitted through electric signals, and stored in electric transistors, each bit a very simple binary state of either 0 or 1. With both the knowledge that every digital content is essentially strings of information the computer can process, and the knowledge that cryptography is used to protect information, it dawns upon us naturally that cryptography can be used to protect digital content.

The technology and science concerning with the protection, distribution, usage, and laws of digital content is often called Digital Rights Management (DRM). There is no common architecture for DRM, as there are many methods and different frameworks offered by different vendors and consultants. But there are standards that must be met and features commonly available in each techniques. These typically include :

1. Encryption of the content in order to prevent unauthorized access

2. Decryption Key Management

3. Access control. An advantage of modern DRM is that the usage rules can easily be adapted to various business models. Access can be restricted to certain users, or a limited time, or a limited number of accesses.

4. Copy control or complete copy prevention. Depending on the usage rules, the DRM can enforce a control on how many times the user can copy the content.

5. Identification and tracking of digital content. Mostly in use when digital content is obtained through physical means, or analog output. The perpetrator can obtain a copy from analog output. Thus, analog copies in general can't be prevented e.g. someone making a recording of a song when it plays on their car radio. It is a nifty addition of feature to have the possibility to identify and trace back analog and digital copies of distributed media. This is usually done through watermarking

7. Secure communications protocol for billing systems and mechanisms.

The techniques of cryptography are many in number the methods diverse in its variety, and computer scientists and engineers all over the world are still churning out new ways of applying cryptography in DRM. To tighten the scope and get an at least general view the writer is trying to achieve in this paper, we shall discuss one of them in general, namely the Fairplay, But first we need to look at basic theories of making a public/private key that has its deep roots in number theory.

3.2. RSA

RSA is a cryptosystem widely known for its use for secure data transmission. The acronym stands for the last names of its founders (Ron Rivest, Adi Shamir, and Leonard Adleman).

The RSA algorithm sets its foundation on the unique properties of prime numbers and it involves three steps: key generation, encryption and decryption. We will proceed with key encryption, then explain how these keys are used to encrypt and decrypt.

For RSA we generate both a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. We generate the keys for RSA in the following way:

1. Choose two distinct large random primes p and q. Generally these should be 100 digits plus.
2. Compute n=pq

This n is used as the modulus for both the public and private keys

3. Choose an integer e such that $1 < e < \varphi(n)$ and $\gcd(e,\varphi(n))=1$ (where $\varphi(n)$ is the Euler φ-function we've been discussing)

e is released as the public key exponent

4. Compute d to satisfy $de=1 \pmod{\varphi(n)}$

Notice that we can always do this because $\gcd(e,\varphi(n))=1$, thus e is in $Z_{\varphi(n)}^{*}$ and hence has a unique multiplicative inverse, namely d.

d is kept as the private key exponent (hence must be kept secret) The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d.

The case of encryption are as follows:

- A transmits her public key (n,e) to B and keeps the private key secret. B then wishes to send message **M** to A.
- He first turns M into a number m < n by using an agreed-upon reversible protocol known as a padding scheme (we will discuss this later). He then computes the cipher text corresponding to:

$$c = m^e \pmod{n}$$

- A can recover m from c by using her private key exponent d by the following computation:

$$m = c^d \pmod{n}$$

- Given m, he can then recover the original message **M**, since the padding scheme is reversible.

- The above decryption works because:

$$c^d = (m^e)^d = m^{ed} \pmod{n}$$

- Now, since ed= 1 + k φ(n), (note this is because ed=1 (modφ(n)),

$$m^{ed} = m^{1 + k\,\varphi(n)} = m(m^k)^{\varphi(n)} = m \pmod{n}$$

The last congruence follows from Euler's theorem which states: If a and n are positive integers with gcd(a,n)=1, then $a^{\varphi(n)}=1 \pmod{n}$. However we already knew this because since gcd(a,n)=1 a is in Z_n^{*} and since the order of this group is φ(n), we get the result. Note: This requires that m be relatively prime to n. Since n=pq, this is only the case if m is a multiple of p or q. Since p and q are usually very large primes this makes it unlikely.

There are many ways to convert a text message into a number. For example you could just sent one letter at a time and denote the letters A-z with the numbers 0-25, then your message **M** is made into a number by converting each letter to its appropriate number (and removing spaces). Note: If you m>n cut it into enough pieces so that each piece (say m_i) is less than n.

Now that we know how one creates a private/public key we can shift our discussion into a DRM system that uses it But because each case of encryption and decryption is different. Let's see how an RSA key generation algorithm actually works.

3.3 RSA Usage

First, let us use the RSA algorithm with numbers easy enough for academic purposes.

Choose two primes, p = 11 and q=13 hence the modulus is n= p × q which is equals to 143. The totient of n will be

$\phi(n)=(p-1)\cdot(q-1)=120$

To generate the public key, choose a random prime number that has a greatest common divisor of 1 with the totient 120, Let's choose 7. So e = 7, and to determine d, the secret key, we need to find the inverse of 7 with $\phi(n)$. This can be done with the Extended Euclidean Algorithm, and hence d = 103. This can be easily verified:

$e\cdot d=1\text{mod}\phi(n)$

$7\cdot 103=721=1\text{mod}120$

To show how the encryption and decryption works, choose a plaintext message, for example, m = 9. The process of encryption is as follows.

Encryption: $m^e \bmod n = 9^7 \bmod 143 = 48$

Now we have the ciphertext 48 for 9, let's call it c. Now when we want to decrypt it we use d we calculated from e and the totient $\phi(n)$ as the exponential of the ciphertext with modular n.

Decryption: $c^d \bmod n = 48^{103} \bmod 143 = 9 = m$

After we've covered the educational example of the usage of RSA algorithm to generate a cryptograhhic key, let's look at a possible real life usage, albeit still simple compared to the one used in DRM.

We try to encrypt the message "attack at dawn". Now, because the RSA algorithm is a mathematical operation, we need to change the sentence into a numerical presentation. Let's use ASCII conversion. "Mr Rinaldi Munir" converted to its ASCII code is

1976620216402300889624482718775150

Now to pick two large primes, p and q. These numbers must be random and not too close to each other. The following numbers are generated with a Rabin-Miller primality test.

p
12131072439211271897323671531612440428472427633701410925634549312301964373042085619324197365322416866541017057361365214171711713797974299334871062829803541

q
12027524255478748885956220793734512128733387803682075433653899983955179850988797899869146900809131611153346817050832096022160146366346391812470987105415233.

With these two large numbers, we can calculate n and totient $\phi(n)$

n
145906768007583323230186939349070635292401872375357164399581871019873438799005358938369571402670149802121818086292467422828157022922076746906543401224889672472407926969987100581290103199317858753663710862357656510507883714297115637342788911463535102712032765166518411726859837988672111837205085526346618740053

$\phi(n)$
145906768007583323230186939349070635292401872375357164399581871019873438799005358938369571402670149802121818086292467422828157022922076746906543401224889648313811232279966317301397777852365301547848273478871297222058587457152891606459269718119268971163555070802643999529549644116811947516513938184296683521280

To look for the public key e, find a number that has a gcd of 1 with $\phi(n)$, we find 65537. So let's use it as the public key. To calculate the private key, use extended euclidean algorithm to find the multiplicative inverse with respect to $\phi(n)$, we obtain

e
65537

d
89489425009274444368228545921773093919669586065884257445497854456487674839629818390934941973262879616797970608917283679875499331574161113854088813275488110588247193077582527278437906504015680623423550067240042466665654232383502922215493623289472138866445818789127946123407807725702626644091036502372545139713.

Now let's encrypt the ASCII-converted "attack at dawn"

Encryption

$(1976620216402300889624482718775150)^e \ mod \ n$

We get the ciphertext

35052111338673026690212423937053328511880760811579981620642802346685810623109850235943049080973386241113784040794704193978215378499765413083646438784740952306932534945195080183861574225226218879827232453912820596886440377536082465681750074417459151485407445862511023472235560823053497791518928820272257787786

Decrypting it would take a lot of time even for a computer to calculate when it knows the private key d (imagine the ciphertext with d as the exponential). That's why RSA is a widely used algorithm for cryptography

Now we bring the focus to a pure RSA based DRM used by Adobe in their products.

3.4. Adobe Digital Experience Protection Technology (ADEPT)

The ADEPT is a DRM cryptosystem developed by Adobe to protect ebooks. In ADEPT, ebooks are encrypted with a book key, each digital copy of the same book is encrypted with the same key that is licensed to a book distributor to use in encryption of their books. Each buyer has his own user key. This key is generated when the user installs Adobe Digital Editions (ADE). When the user buys an ebook, ADE downloads the encrypted ebook from the distributor, and ADE obtains a license through a process called fulfillment.

The fulfillment process involves the RSA-generated user key which is different for each book, unlike the book key from the distributor. The process is fulfilled when ADE sends a decryption attempt that is confirmed on the distributors' side of the process.

3.5 Fairplay

Fairplay was first introduced by Apple in 2003, to coincide with the release of their iTunes Online Music Store, Songs purchased through the store have built in DRM through a technology called Fairplay built in to QuickTime Software which is the multimedia foundation of iTunes music player. The system has caused much controversy in its limitations that downloaded songs may only be played on hardware running Apple's software.

Media downloaded from the online store consists of an encrypted AAC audio stream residing in an mp4 container. In order to download and decrypt songs, the user needs to create an account at the iTunes Store and authorize a computer using that account to run the iTunes client software. Then, Apple assigns a globally unique identification for the computer that has been authorized. The user can authorize up to five computers at once to use with the same iTunes account.

The system uses two keys:
1.A master key that is used to decrypt and playback the audio content. It is embedded in the mp4.
2.A user key that is used to decrypt the master key in the audio file.

The keys are generated through a computer-adapted form of RSA public/private key scheme generation. Decryption happens in several stages: The first step is to produce an initialization vector for decrypting the area holding the master key. This vector is acquired by applying a hash function to the user id and a special initialization field in the file. When the master key is decrypted, we use it along with a second initialisation vector that has become available through decryption, to decrypt each sample of audio data.

When a user makes a purchase, the following takes place

-A random user key for that specific purchase is generated
-The plaintext file is downloaded
-The master key in the file is encrypted using the user key

The user needs to authorize all computers and devices that will play the file. When authorized, all user keys associated with the particular user is transferred from Apple's servers to the user's authorized computer. However, the use of the RSA algorithm happens locally in the user's iTunes client.

3.6. Diffie-Hellman Key Exchange (DH)

Even though we have solved the problem of data protection, it would be meaningless if the key that unlocks the encryption easily leaks when transmitted through an insecure communication channel. So although we have encrypted the data itself, there needs to be a way to transfer the key safely when we intend to give it to the correct recipient.

The DH scheme was first proposed by Whitfield Diffie and Martin Hellman in 1976, it is one of the first key exchange algorithms that is still used to this day.. Suppose there are two parties A and B, with C trying to snag the key through the insecure communications channel.

- The first step is for A and B to agree on a large prime p and a nonzero integer $g \bmod p$. the p and g has no need to be kept secret, so C might know them.
- Now A is to pick a secret integer a that is kept secret, even to B, B picks another integer b that is also kept secret to A.
- A computes $X \cong g^a \bmod p$
- B computes $Y \cong g^b \bmod p$
- A gives the X to B and B gives Y to A
- A computes $X' \cong Y^a \bmod p$
- B computes $Y' \cong X^b \bmod p$
- Now X' and Y' should be the same, because

$$X' \cong X^a \cong (g^b)^a \cong g^{ab} \cong Y^b \cong Y' \pmod p$$

- This shared value is now the encrypted key that they can both decrypt. C can only know the shared value but will be useless since C doesn't know the secret numbers a and b

Now we do it with an example

- A and B agree to use the prime number p = 941 and primitive root g = 627
- A choose secret key a = 347 and computes

$$X = 390 \cong 627^{347} (mod\ 941)$$

- B chooses secret key $\boldsymbol{b}$ **=** 781 and computes

$$Y = 691 \cong 627^{781} (mod\ 941)$$

- A gives X to B and B gives Y to A, this is often done through an insecure communication so C can know their values but useless since a and b is kept secret
- Now they can both compute

$$470 \cong 627^{347.781} \cong X^b \cong Y^a$$

- 470 is the shared secret number without this number itself ever going through a communication channel and can be used as a symmetric key to an encryption.

The Diffie-Hellman Key Exchange proves to be a simple but effective method of sharing a value without the value itself ever going through transmission, and this is used to support most symmetric DRM cryptosystems in distributing the key to decrypt the content.

IV. CONCLUSION

Number theory is a field of discrete mathematics commonly used in information technology and computer science that studies integers, their properties, and their relation to other integers

Digital Rights Management is useful in protecting digital information through the use of very flexible algorithms, and the possibilities to keep the file safe are endless. Three key components is needed to build a digital content protection system through cryptography, the first is generating a key, whether symmetric or asymmetric between the sender and recipient, second is encryption done on the sender side, and the third is the decryption consumers do when the encrypted information reaches them.

The algorithm commonly found in cryptosystems in DRM, is the RSA, an algorithm that has its roots in modular arithmetic and unique properties of prime numbers, RSA is used in ADEPT and Fairplay.

There must be a way to make the transmitting of the cryptosystem's key safe, and we can do it also with cryptography. The Diffie-Hellman Key Exchange algorithm is one of the first ones and is still widely used in in supporting DRM.

REFERENCES

[1] G. A. Miller and J. A. Selfridge, "A Course on Number Theory," *The American Journal of Psychology*, vol. 63, no. 2, pp. 176–185, 1950.

[2] Xiao Zhang, "A Survey of Digital Rights Management Technologies.".Stanford.2010.

[3] "Analysing ADEPT (Adobe Digital Experience Protection Technology) | Jaap-Henk Hoepman - on security, privacy and..." [Online]. Available: http://blog.xot.nl/2012/04/12/analysing-adept-adobe-digital-experience-protection-technology/. [Accessed: 15-Dec-2013].

[4] M. Persson and A. Nordfelth, *Cryptography and DRM*. Uppsala Universitet, 2008.

[5] J. He and H. Zhang, "Digital Right Management Model Based on Cryptography and Digital Watermarking," 2008, pp. 656–660.

[6] Avi Kak, *Elliptic Curve Cryptography and Digital Rights Management*. 2013.

[7] “How RSA Works With Examples.” [Online]. Available: http://doctrina.org/How-RSA-Works-With-Examples.html. [Accessed: 15-Dec-2013].

[8] “Modern Cryptography: Theory and Applications.” [Online]. Available: http://www-cs-faculty.stanford.edu/~eroberts/courses/soco/projects/2004-05/cryptography/drm.html. [Accessed: 09-Dec-2013].

[9] “Number Theory and Cryptography.” [Online]. Available: http://www.math.cornell.edu/~mec/2008-2009/Anema/numbertheory/rsa.html. [Accessed: 15-Dec-2013].

[10] E. Arsenova, *Technical aspects of digital rights management*. 2008.

[11] “The Uses and Limits of Cryptography in Digital Rights Management.” [Online]. Available: http://www.info-mech.com/drm_cryptography.html. [Accessed: 09-Dec-2013].

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 17 Desember 2013

ttd

Adhika Sigit Ramanto - 13512060